

**Prepared Remarks of  
Michehl R. Gent, President and Chief Executive Officer  
North American Electric Reliability Council**

**Hearing Before the United State's Senate  
Subcommittee on Technology, Terrorism, and Government Information**

**July 25, 2001**

**THE ELECTRICITY SECTOR RESPONSE TO  
THE CRITICAL INFRASTRUCTURE PROTECTION CHALLENGE**

My name is Michehl R. Gent, and I am President and Chief Executive Officer of the North American Electric Reliability Council (NERC). I am responsible for directing NERC's activities within the industry and with the federal government as these activities relate to terrorism and sabotage of the electric systems of North America. Since mid-1998, these activities include critical infrastructure protection.

NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. It works with all segments of the electric industry — investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; and power marketers — as well as customers to “keep the lights on” by developing and encouraging compliance with rules for the reliable operation of these systems. NERC comprises ten Regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

In my testimony I will discuss NERC's relationship with the National Infrastructure Protection Center and several related critical infrastructure protection programs that NERC participates in: Critical Infrastructure Protection Working Group; Indications, Analysis, and Warnings Program; Electricity Sector Information Sharing and Analysis Center; Critical Infrastructure Protection Planning; and Partnership for Critical Infrastructure Security.

**Summary**

NERC has an excellent working relationship with the National Infrastructure Protection Center (NIPC). NERC and the electric industry worked closely with NIPC for about two years to develop a voluntary, industry-wide physical and cyber security indications, analysis, and warning (IAW) reporting procedure. This program provides NIPC with information that when combined with other intelligence available to it will allow NIPC to provide the electric industry with timely, accurate, and actionable alerts and warnings of imminent or emerging physical or cyber attacks. A high degree of cooperation with NIPC is possible because the industry has a long history of working with local, state, and federal government agencies. In addition, the NERC Board of Trustees in the late 1980s resolved that each electric utility should develop a close working relationship with its local Federal Bureau of Investigation (FBI) office, if it did not already have such a relationship. The Board also said the NERC staff should establish and maintain a working relationship with the FBI at the national level.

The Indications, Analysis, and Warnings Program (IAW) reporting procedure is modeled on an existing electric system disturbance reporting procedure in which electric utilities report system disturbances meeting predefined criteria to the U.S. Department of Energy. A pilot IAW program was field tested in one NERC Regional Reliability Council in the fall of 1999 and winter 1999/2000. The

program was refined and rolled out to the industry via three workshops held during the fall of 2000 and winter 2000/2001. A comprehensive communications program is being developed to bring this program to the attention of those industry entities that were not able to participate in the workshops.

### **NERC National Infrastructure Security Activities**

NERC has served on a number of occasions during the past decade as the electric utility industry (electricity sector) primary point of contact for issues relating to national security. Since the early 1980s, NERC has been involved with the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Year 2000 rollover impacts, and now the threat of cyber terrorism. At the heart of NERC's efforts has been a commitment to work with various federal government agencies such as the U.S. National Security Council, U.S. Department of Energy (DOE), and FBI to reduce the vulnerability of interconnected electric systems to such threats.

The report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to a May 1998 Presidential Decision Directive (PDD-63). PDD-63 called for government agencies to become involved in the process of developing a National Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical systems through public-private partnerships. The PCCIP specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. In September 1998, Secretary of Energy Bill Richardson wrote to NERC Chairman Erle Nye seeking NERC's assistance, on behalf of the electricity sector, in developing a program for protecting the nation's critical electricity sector infrastructure. Responding to the (DOE) critical infrastructure protection initiative, NERC agreed to participate as the electricity sector coordinator.

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison, worked through its Infrastructure Assurance Outreach Program to perform an information assurance assessment for a small number of nodes on NERC's industry information system. The purpose of this assessment was to help NERC and the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. A second follow-on information system assessment was begun in late 2000 and will be completed shortly. The product of this study will be recommendations that will form the basis of a draft NERC policy on information assurance. In addition, to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America, DOE has provided clearances for a number of industry personnel and clearances for other key industry personnel are anticipated. These clearances compliment those obtained from the Federal Bureau of Investigation (FBI) as a result of encouragement by NIPC, as discussed below.

### **Critical Infrastructure Protection Working Group**

After several exploratory scoping sessions with DOE and NIPC, NERC created a Critical Infrastructure Protection (CIP) Forum to evaluate sharing cyber and physical incident data affecting the bulk electric systems in North America. The meetings of this group were widely noticed and the participants included all segments of the electric utility industry and representatives from several government agencies including the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, DOE, and NIPC. As a result of the groups' deliberations, NERC created a permanent group within the NERC committee structure — the Critical Infrastructure Protection Working Group (CIPWG). This working group reports to NERC's Operating Committee. It has Regional Reliability Council and industry sector representation as well as participation by the CIAO in the Department of Commerce, DOE, and NIPC.

## **Indications, Analysis, and Warnings Program**

One of the first tasks of the Critical Infrastructure Protection Forum was to develop the incident data types and event thresholds to be used in an information-sharing program with NIPC. Information sharing (electronic and telephone) mechanisms have been developed for use by electric transmission providers, generation providers, and other industry entities for reporting on a voluntary basis to both NIPC and NERC. Assessments, advisories, and alerts prepared by NIPC (with NERC's support), based on the data provided by the electric and other industry sectors and government sources, will be stated in an actionable manner and will be transmitted to electric industry entities. This process was tested successfully within one Reliability Council Region during the fall 1999 and winter 1999/2000. Because some of the analyses involve classified information, U.S. government security clearances have been obtained by key industry personnel and NERC staff members. Other electric industry personnel are in the process of obtaining security clearances.

The electric industry Indications, Analysis, and Warnings Program, which evolved from this work (Attachment A), was presented to the NERC Operating Committee in July 2000 for discussion and approval. The Operating Committee approved a motion to implement the program; initial emphasis is on reporting by security coordinators and control areas. Individual electric utilities, marketers, and other electricity supply and delivery entities are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings and related materials. Workshops were conducted during the fall 2000 and winter 2001 to provide program details to the industry. A more comprehensive communications program is being developed by CIPWG to encourage broader industry participation in the program. NERC views the Indications, Analysis, and Warnings Program as a voluntary first step toward preparing the electricity sector to meet PDD-63 objectives.

## **Electricity Sector Information Sharing and Analysis Center**

The PCCIP recommended that each of the critical sectors establish an Information Sharing and Analysis Center (ISAC) to help protect the infrastructures from disruption arising from coordinated intrusion or attack. The ISACs would gather incident data from within their respective sectors, perform analyses to determine potential malicious intent, share findings with other ISACs (private and government) in a manner that assures, as required, target identity protection, and disseminate actionable warnings so appropriate action can be taken within each sector. ISACs would serve as points of contact between sectors to facilitate communications, especially during a time of stress. ISACs would study cross sector interdependencies to better understand and be prepared for the possible impacts of an "outage" of one sector on another.

The CIPWG has endorsed, and NERC has accepted, the naming of NERC as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The functions performed are essentially the same as those functions that have been required of NERC for physical sabotage and terrorism. The ES-ISAC's duties are:

1. Receive voluntarily supplied incident data from electric industry entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.
3. Assist the NIPC personnel during its analyses on a cross private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts and other related materials to all those within the electric industry who wish to participate.

The ES-ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will likely request support for a 24-hour, seven days a week

staffed facility. To this end, NERC also is exploring the feasibility of forming a joint ISAC with other sectors. NERC has established relationships with the other existing ISACs through the Partnership for Critical Infrastructure Security (see below) and will establish relationships with other ISACs as they form.

### **Critical Infrastructure Protection Planning**

The CIPWG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the electric industry (Attachment B). Separate business cases have been prepared for Chief Executive Officers, Chief Operating Officers, Chief Information Officers, and a NERC general overview (Attachments C, D, E, and F). The purpose of the business case is to persuade industry participants of the need to report cyber intrusion incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPWG has developed a basic and fairly comprehensive plan to address CIP. The working group was concerned about generating an overly prescriptive plan too early in the process and has proceeded with a format that can assist in developing each entity's own plan. The prototype plan, which still is undergoing industry review, addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, reconstitution, and interdependencies between and among sectors.

The essence of this "Approach to Action" is being considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government. Richard Clarke, Special Assistant to the President and National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, has discussed the importance of establishing and maintaining a National Plan to the health of the government and private sectors, companies, and the nation. Version 1.0 of the Plan did a good job covering the threats and the government response, but it did not detail private sector response. The need for private sector participation is engendered by the fact that the government lacks private sector expertise and needs private sector "buy in" to CIP initiatives. The National Plan version 2.0, which will include private sector input, is scheduled for fall 2001.

### **Partnership for Critical Infrastructure Security**

The Partnership for Critical Infrastructure Security (PCIS) was proposed in late 1999 by members of several private sectors; the PCIS is supported by CIAO and the U.S. Chamber of Commerce. Earlier this year, it established itself as a not-for-profit organization and elected a Board of Directors and company officers. NERC participates in PCIS and I serve as its Secretary.

The PCIS Mission:

Coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

The PCIS held two general forums in 2000 and one so far this year. It is planning a second general forum on September 6–7, 2001. The PCIS has formed six active working groups: Interdependency Vulnerability Assessment and Risk Management; Information Sharing, Outreach and Awareness; Public Policy and Legislation; Research and Development and Workforce Development; Organization Issues and Public-Private Relations; and National Plan. The opportunities presented by PCIS include gaining a better perspective of the sector interdependencies, facilitating ISAC formation, and sharing of common research and development efforts.